Onions in the Cloud Make the CISO Proud

Wes Lambert
@therealwlambert
DEF CON Cloud Village 2021

Agenda

- The Cloud
- Introduction to Security Onion
- Security Onion in the Cloud

The Cloud - Data Storage/Transit

- **Amazon Web Services**
  - S3 Buckets
  - Dynamo DB
- **Azure**
  - Blobs
  - Event Hubs
- **Google Cloud Platform**
  - Storage Buckets
  - Cloud Datastore/Filestore
- **Application/Network Traffic**

The Cloud - Data Exploited/Abused

AWS (Amazon Web Services)

- S3Scanner
  - scan for open S3 buckets
- Pacu
  - AWS exploitation framework

https://github.com/sa7mon/S3Scanner

https://github.com/RhinoSecurityLabs/pacu

The Cloud - Data Exploited/Abused

Azure

- MicroBurst
  - Azure Services discovery
  - weak configuration auditing
  - post exploitation actions

https://github.com/NetSPI/MicroBurst

The Cloud - Data Exploited/Abused

GCP (Google Cloud Platform)

- GCP-IAM-Privilege-Escalation
  - Permissions enumeration
  - Exploits for privilege escalation
- GCPBucketBrute
  - Enumerate Google storage buckets, determine access
  - Determine if privesc'able

https://github.com/RhinoSecurityLabs/GCP-IAM-Privilege-Escalation

The Cloud - Credentials (AWS)

- **Account passwords phished via email**
  - IAM account credentials
  - Root account credentials
- **Access keys**
  - Control AWS servers without user/pass
  - Obtained via phish or some other method

The Cloud - Credentials (AWS)

- **Privilege Escalation**
  - Creating new policy versions
  - Creating new user access keys
  - Adding malicious Lambda layer to existing function

https://github.com/RhinoSecurityLabs/AWS-IAM-Privilege-Escalation

Monitoring Challenges

Challenges with NSM in the Cloud

- VXLAN encapsulation (AWS)
  - We can record it, but can our applications handle it?
- Segmentation
- Ephemerality
  - Services in the cloud frequently spin up/down
- In some cases, no native (scalable) mechanism for network monitoring (Azure)

Security Onion - Introduction

- Created by Doug Burks in 2008
- Free and open platform for intrusion detection, enterprise security monitoring, and log management
- Can be installed from a Centos 7-based ISO image, or packages on top of Ubuntu 18.04, or Centos 7

Security Onion: Alert Data

- Wazuh - HIDS
- Suricata - NIDS
- Playbook – Sigma
- Strelka - YARA

		Count	rule.name
🔔	⚠	2	Suspicious Use of Procdump
🔔	⚠	1	Sysmon - Suspicious Process - svchost.exe
🔔	⚠	1	Whoami Execution
🔔	⚠	3	Windows Application error event

rule.name
ET POLICY Signed TLS Certificate with md5W
ET POLICY curl User-Agent Outbound
ET DNS Query for .su TLD (Soviet Union) Ofte
ET DNS Reply Sinkhole - sinkhole.cert.pl 148.81.111.111
ET INFO DYNAMIC_DNS Query to a Suspicious no-ip Domain
ET INFO Packed Executable Download

Security Onion: Metadata

Network Metadata

- Suricata/Zeek
  - DNS
  - HTTP
  - SMB
  - TLS
  - and much more

Security Onion: Full Content Data

Full Content Data (PCAP)

Google Stenographer

Complete transcript

```
POST /mor13/DESKTOP-LOGAN-1_W10019042.94A2671ED67E1F2CADDA5F89B8AB9E64/83/ HTTP/1.1
Accept: */*
Content-Type: multipart/form-data; boundary=----------DQIBOCMQNVNDHVNG
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E)
Host: 186.47.209.222:443
Content-Length: 318
Connection: Close
Cache-Control: no-cache

----------DQIBOCMQNVNDHVNG
Content-Disposition: form-data; name="formdata"

{"PasswordText":["P@ssw0rd-W0lverine"]}----------DQIBOCMQNVNDHVNG
Content-Disposition: form-data; name="billinfo"

{]}----------DQIBOCMQNVNDHVNG
Content-Disposition: form-data; name="cardinfo"

{]}
----------DQIBOCMQNVNDHVNG--
HTTP/1.1 200 OK
connection: close
server: Cowboy
date: Wed, 13 Jan 2021 20:52:21 GMT
content-length: 3
Content-Type: text/plain

/1/
```

PCAP interface in SOC

Security Onion: Supplementary Data

Filebeat Modules

https://docs.securityonion.net/en/latest/filebeat.html#modules

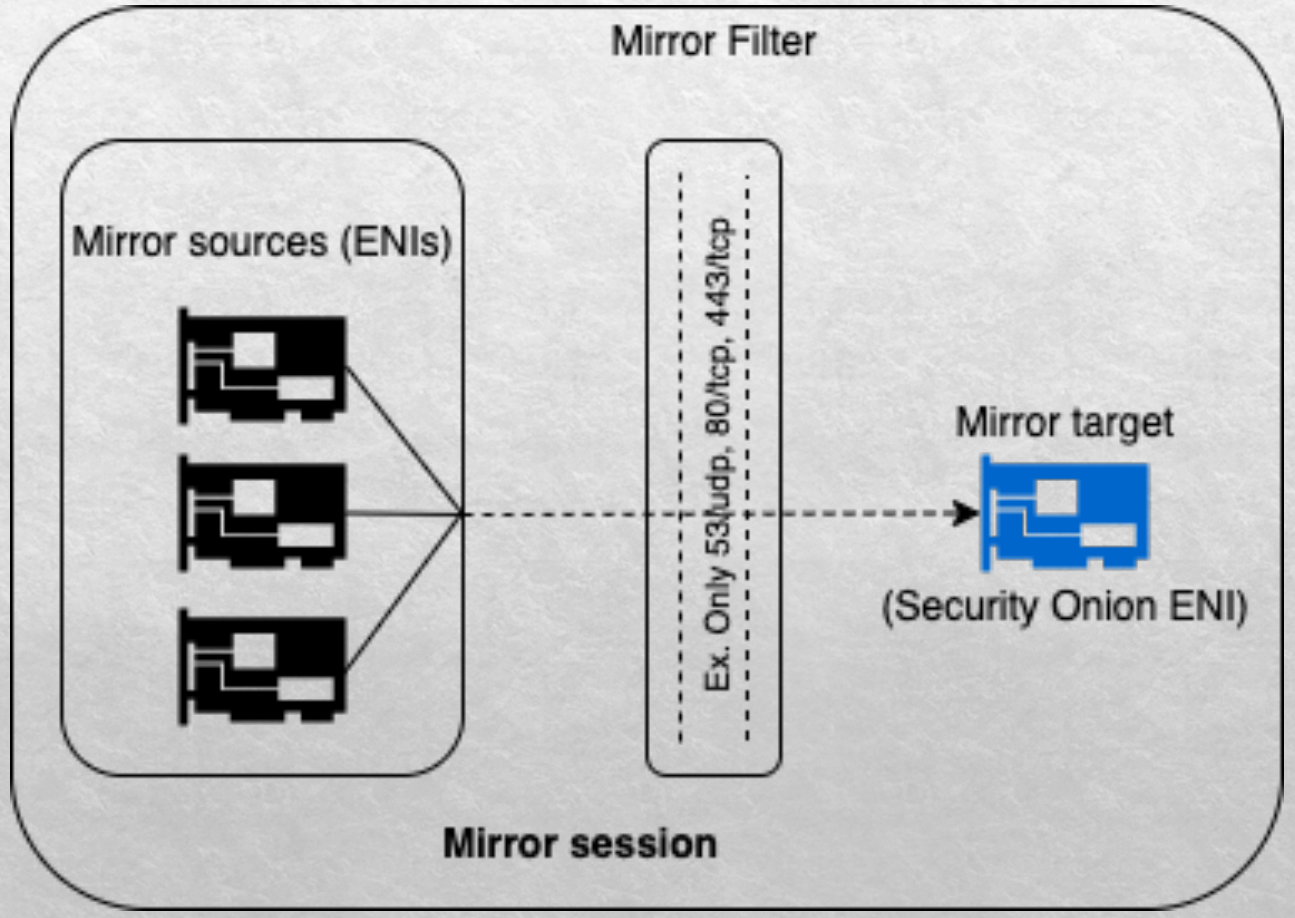
Host Data

(native, as well as shipping Sysmon/Windows Event Logs)

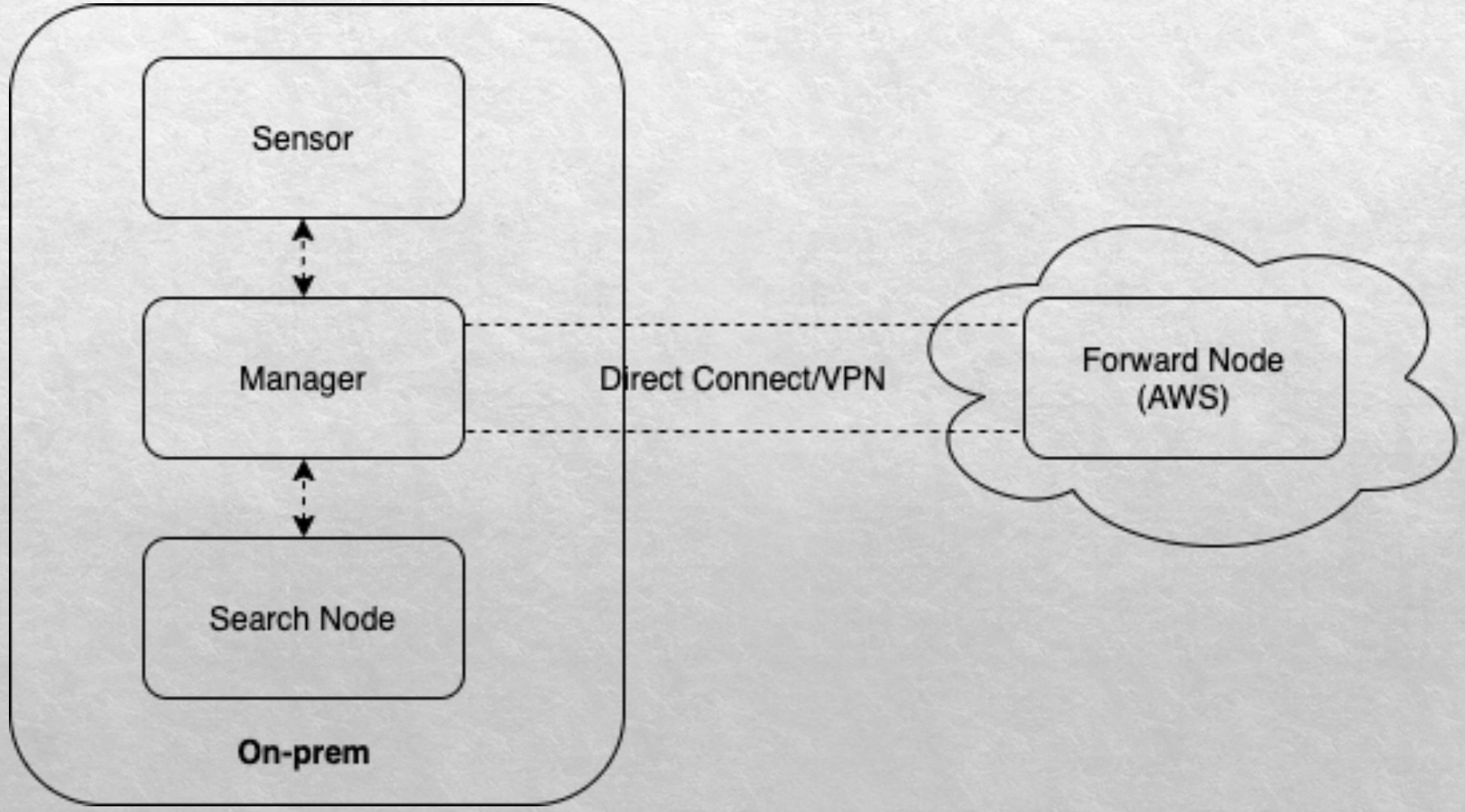
- Osquery
- Winlogbeat
- Wazuh

Traffic Mirroring

Security Onion: AWS Traffic Mirroring

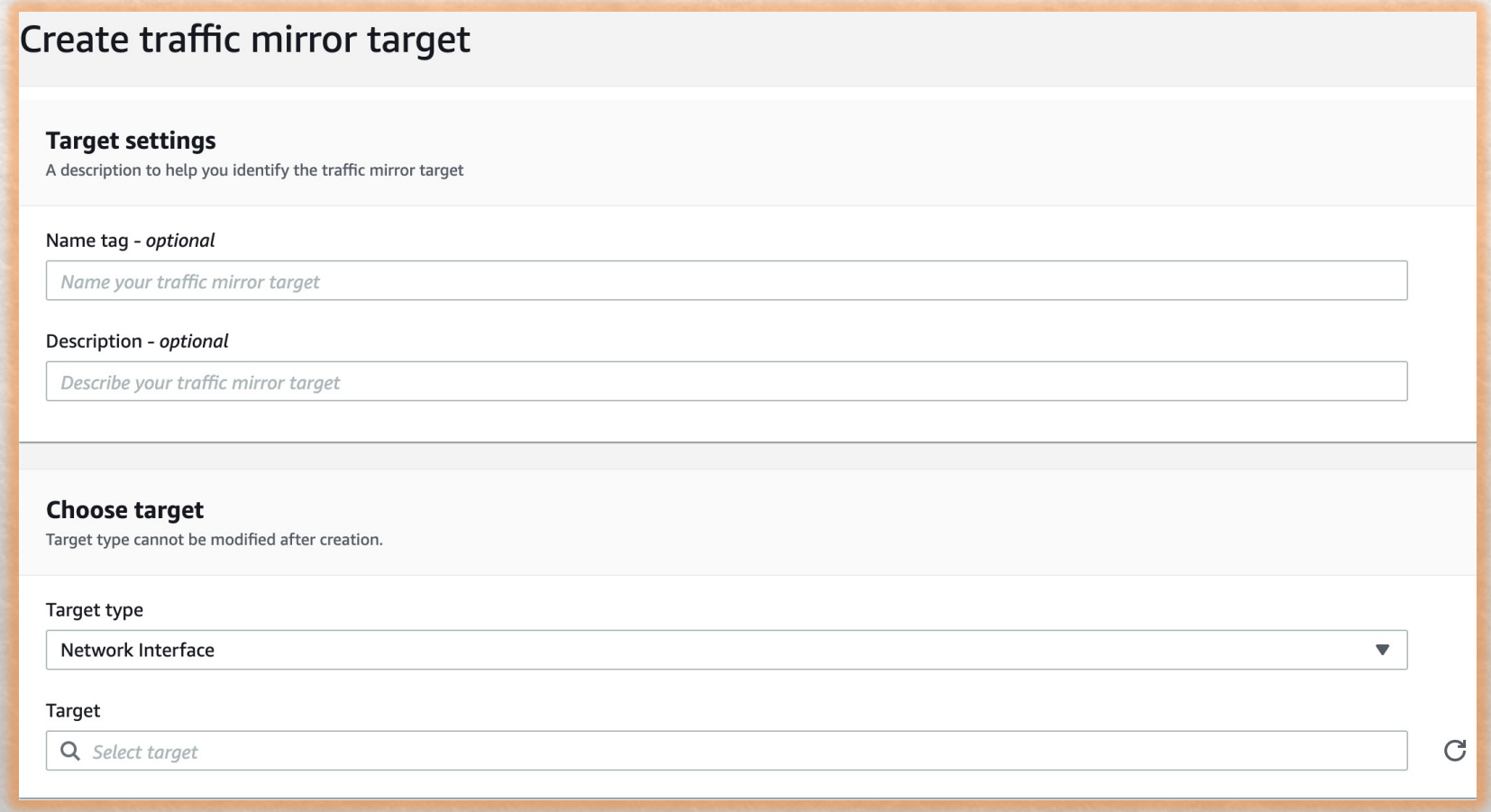


Security Onion: AWS Cloud Node

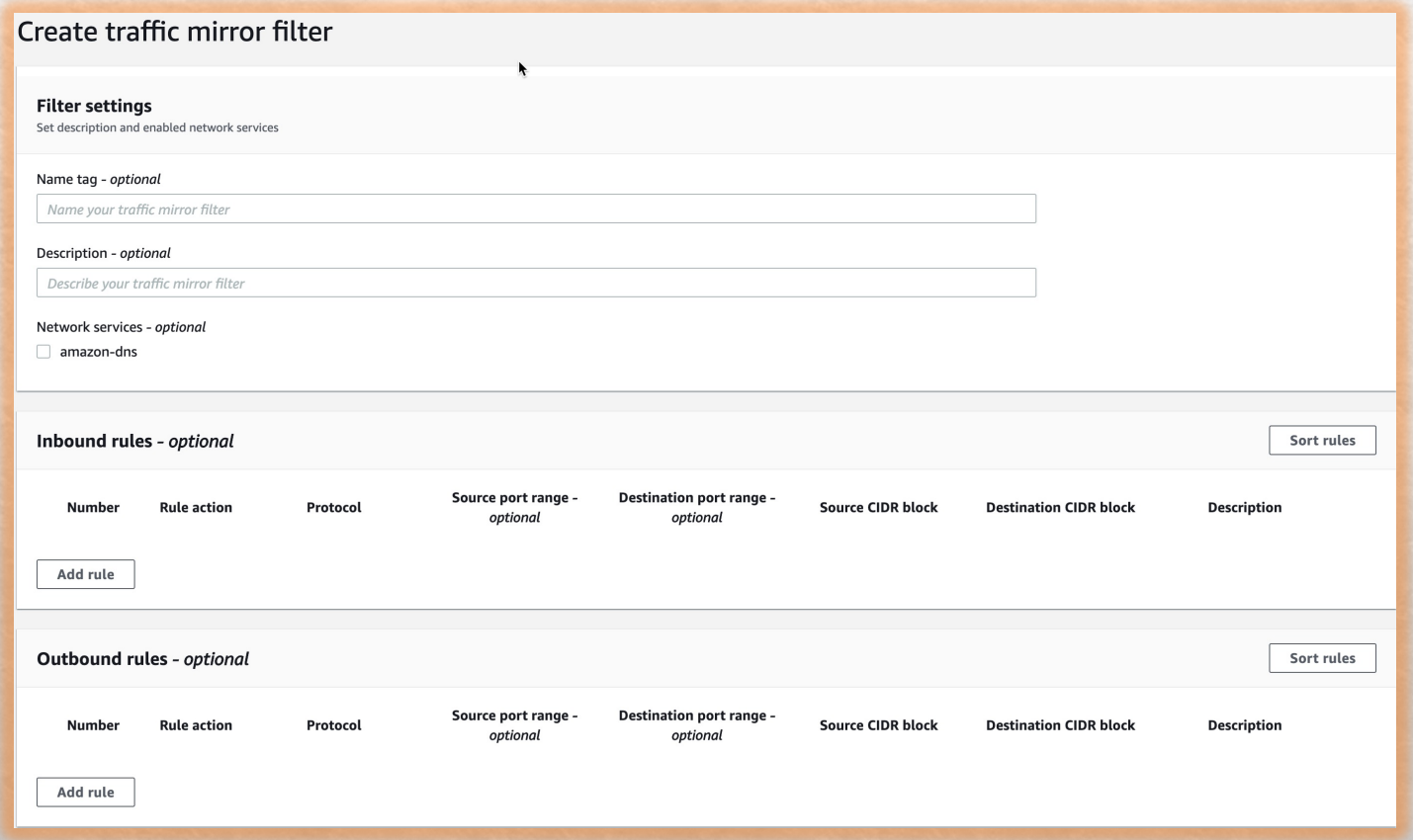


Traffic Mirror Target

Define the target interface where we would like to send mirrored traffic



Traffic Mirror Filter



Define the protocols/traffic to be mirrored

Filter out any unwanted traffic

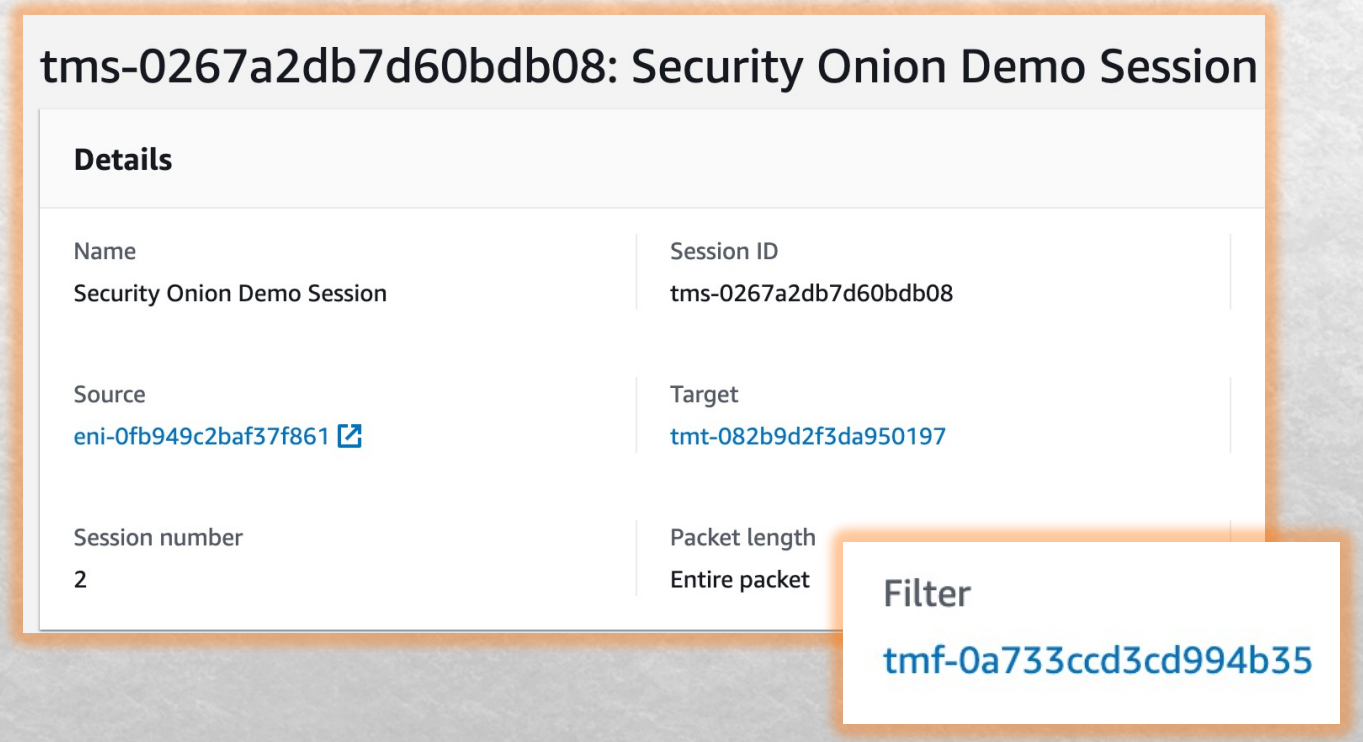
Traffic Mirror Session

Mirror Session is comprised of:

Source interface (to be mirrored)

Target Interface

Mirror Filter



Security Onion: Traffic Mirroring Notes

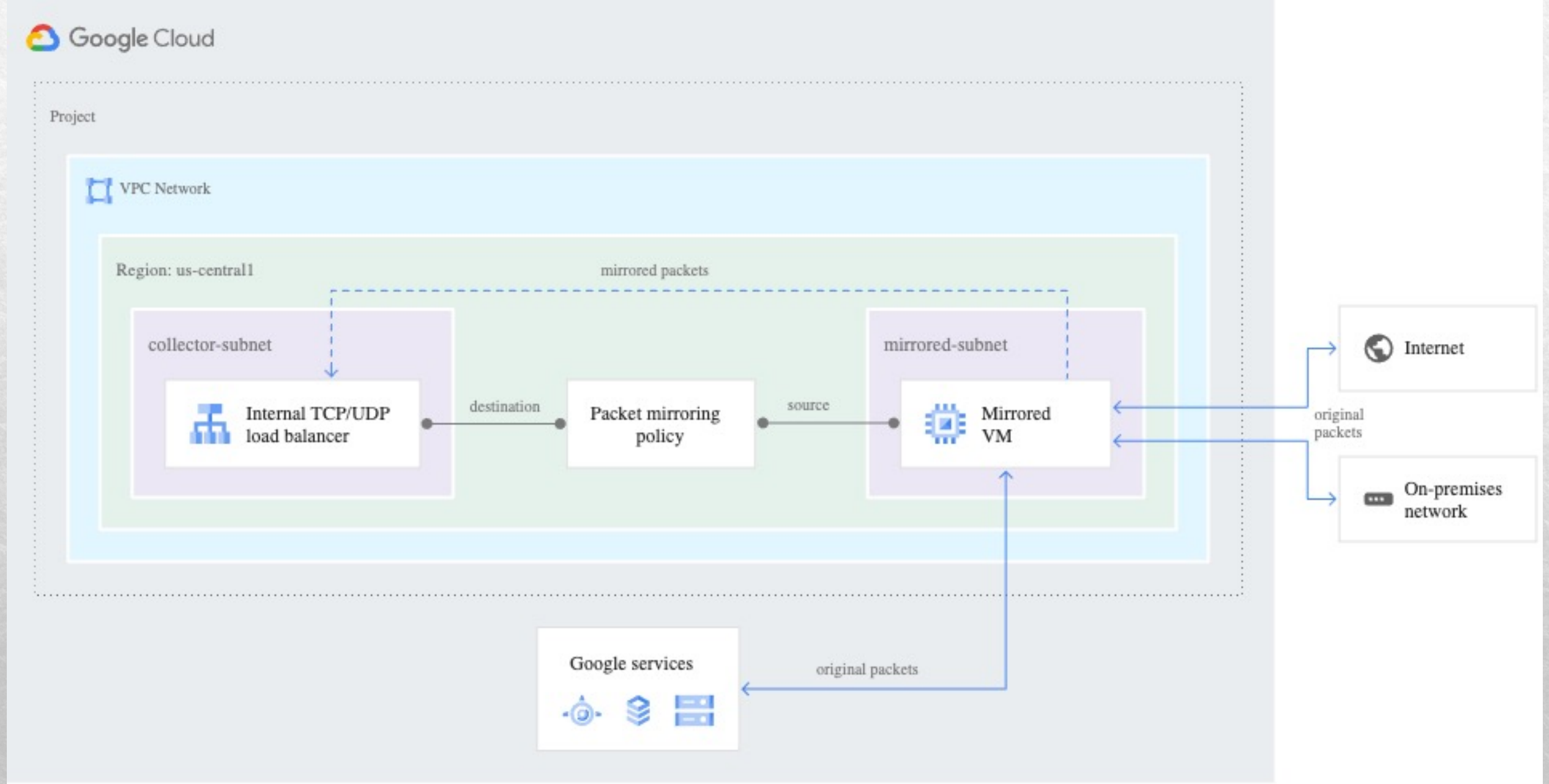
- Suricata (4.1.5+) can natively decapsulate VXLAN
- Zeek (3.0.x+) can natively decapsulate VXLAN
- Traffic Mirroring is capable with only Nitro-based instances

https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-considerations.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html#ec2-nitro-instances

GCP

GCP Packet Mirroring Components

- **Packet mirroring policy** to determine which instances/interfaces participate in traffic mirroring and traffic is mirrored from instance interfaces
- **TCP/UDP Load Balancer** to distribute traffic to a group of instances/interfaces within a collector destination
- **Collector destination** is an instance group where traffic is sent by TCP/UDP load balancer



GCP Packet Mirroring

https://cloud.google.com/vpc/docs/packet-mirroring

GCP Packet Mirroring - Notes

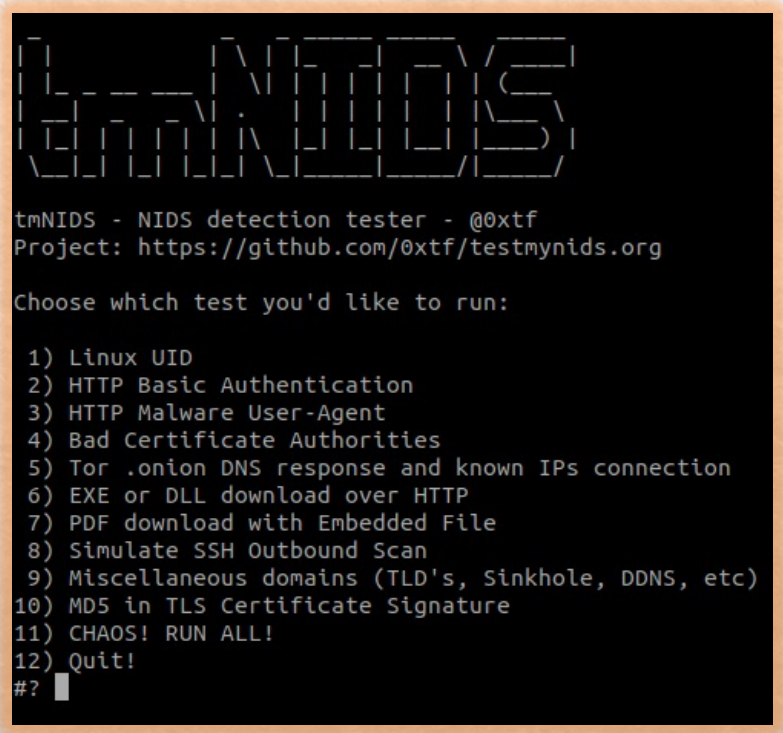
An instance in GCP CANNOT have more than one network interface that resides within the same network/VPC.

This means that the Security Onion management interface (eth0) should reside in it’s own network/VPC.

tmNIDS

- Open-source
- Written by Tiago Faria, 3CoreSec (0xtf)
- Test alerting for cloud or on-premises NSM quickly and easily

ET SCAN Potential SSH Scan OUTBOUND
ET DNS Query for .su TLD (Soviet Union) Often Malware Related
ET DNS Reply Sinkhole - sinkhole.cert.pl 148.81.111.111
ET INFO DYNAMIC_DNS Query to a Suspicious no-ip Domain
ET POLICY DNS Query for TOR Hidden Domain .onion Accessible Via TOR
ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted
ET TOR Known Tor Exit Node Traffic group 35
ET TOR Known Tor Exit Node Traffic group 75
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 162
ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 227



https://github.com/0xtf/testmynids.org

3CoreSec AutoMirror

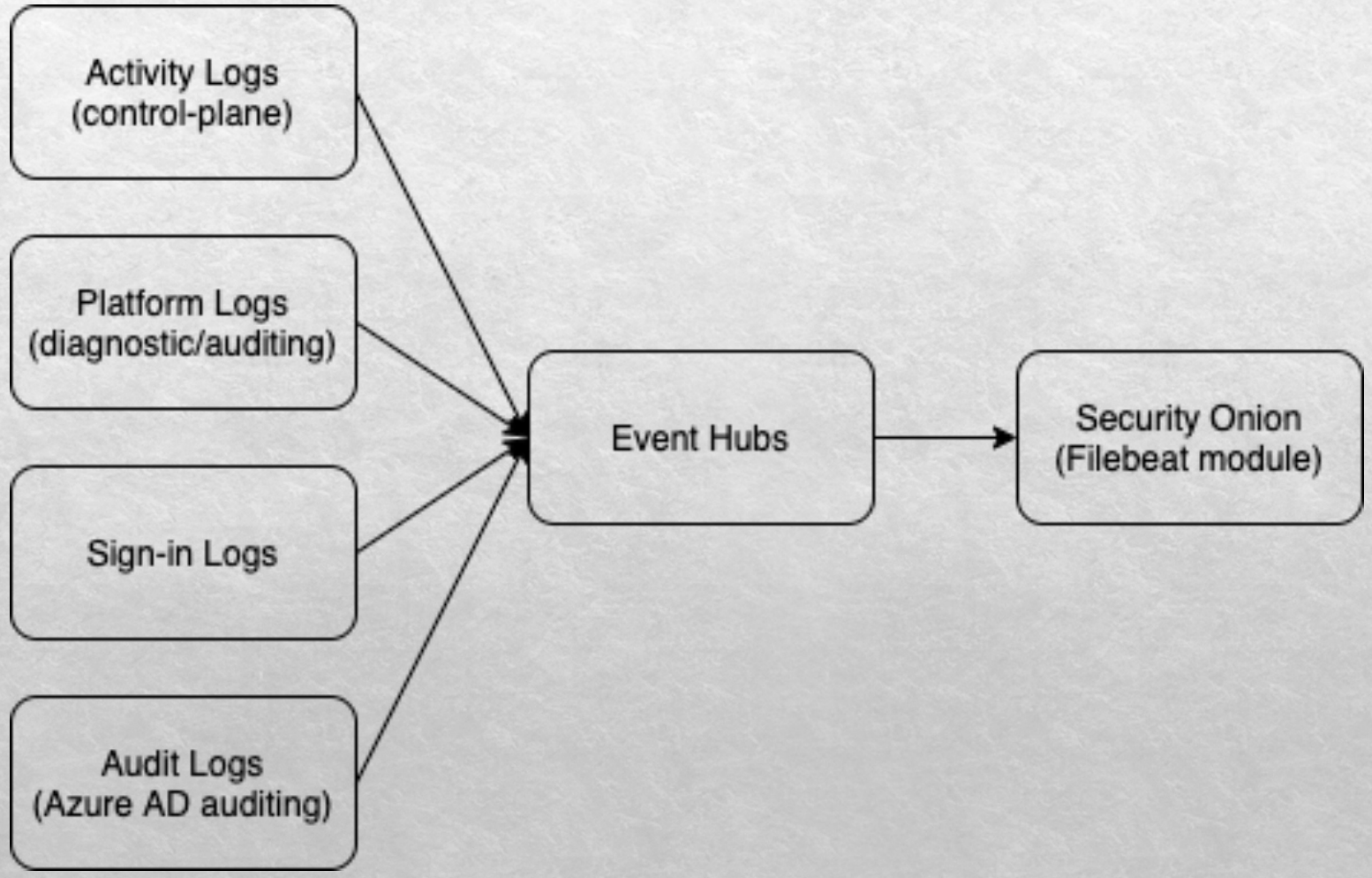
- Open-source
- AWS Lambda function/serverless app
- Quickly and easily facilitate cloud NSM
- Monitors EC2 instances
  - If instances created with **Mirror=True** tag (and if instance is a supported type), their interfaces will be added to a VPC mirror session
  - Also works for instances that are tagged, then restarted

https://github.com/3CORESec/AWS-AutoMirror

Lab

Cloud Logs

Security Onion: Azure Data



Security Onion: Azure Configuration

- Create a resource group
- Create an Event Hubs namespace
- Create an event hub
- Stream logs to the event hub
- Use the **azure** Filebeat module to ingest data into Security Onion

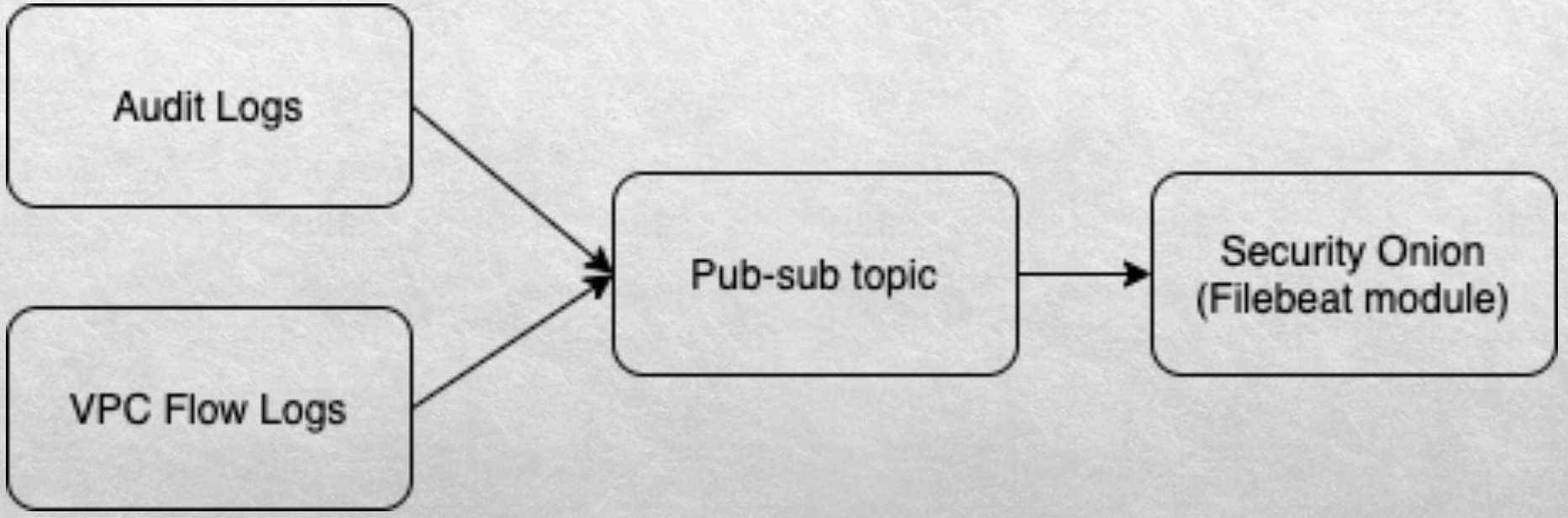
https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-create

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-azure-monitor-stream-logs-to-event-hub

https://docs.securityonion.net/en/latest/filebeat.html#modules

https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-module-azure.html

Security Onion: GCP Data

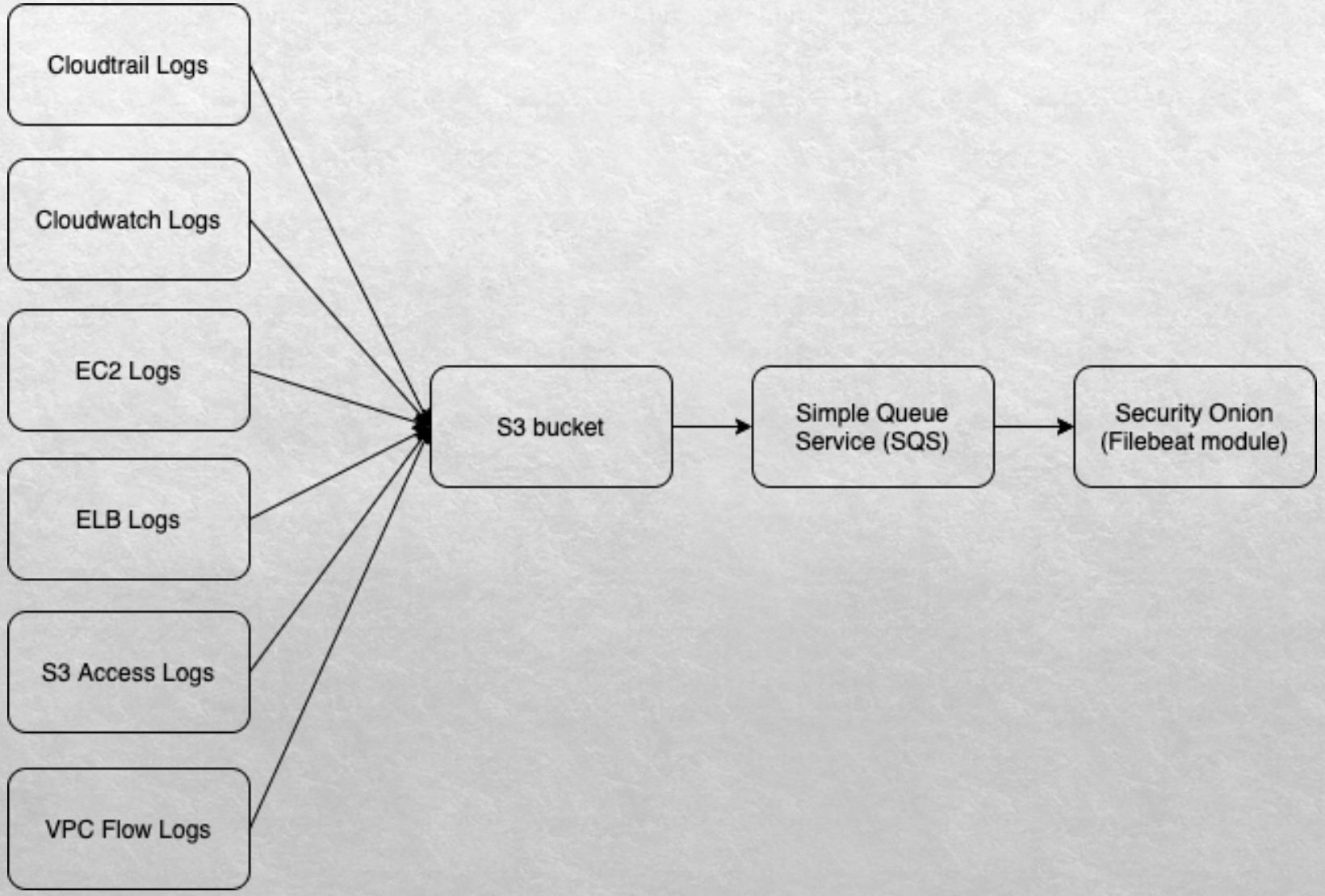


Security Onion: GCP Configuration

- Configure Audit (IAM&Admin->Default audit config))
- Configure VPC flow logs (VPC network -> Flow logs -> Configure)
- Logs Viewer -> Create Sink -> Pub/Sub topic
- Create subscription
- Create service account with the Pub/Sub Editor role
- Configure Filebeat module in Security Onion

https://docs.securityonion.net/en/latest/filebeat.html#modules
https://www.elastic.co/blog/monitoring-google-cloud-with-the-elastic-stack-and-google-operations

Security Onion: AWS



Security Onion: AWS Cloudtrail Configuration

- Configure Cloudtrail to send to S3 bucket (also configure S3 bucket notify SQS)
- Filebeat pulls from SQS/S3 and processes into Elastic Stack on Security Onion
- Sift through data in Hunt and/or alert internally/centrally using

https://docs.securityonion.net/en/latest/filebeat.html#walktrough-aws-cloudtrail-logs

Lab

Additional Tools

vxlan2pcap

- Convert VXLAN-encapsulated PCAP to be readable by tools that do not support VXLAN encapsulation:

./vxlan2pcap vxlan.pcap out.pcap

```
wlambert@dev:~$ sudo tcpdump -nnr vxlan.pcap -c 3
reading from file vxlan.pcap, link-type EN10MB (Ethernet)
15:20:32.675392 IP 192.168.56.11.39924 > 192.168.56.12.4789: VXLAN, flags [I] (0x08), vni 123
ARP, Request who-has 10.0.0.2 tell 10.0.0.1, length 28
15:20:32.675732 IP 192.168.56.12.40908 > 192.168.56.11.4789: VXLAN, flags [I] (0x08), vni 123
ARP, Reply 10.0.0.2 is-at 4a:7f:01:3b:a2:71, length 28
15:20:32.676047 IP 192.168.56.11.48134 > 192.168.56.12.4789: VXLAN, flags [I] (0x08), vni 123
IP 10.0.0.1 > 10.0.0.2: ICMP echo request, id 3389, seq 1, length 64
wlambert@dev:~$ sudo tcpdump -nnr out.pcap -c 3
reading from file out.pcap, link-type EN10MB (Ethernet)
15:20:32.675392 ARP, Request who-has 10.0.0.2 tell 10.0.0.1, length 28
15:20:32.675732 ARP, Reply 10.0.0.2 is-at 4a:7f:01:3b:a2:71, length 28
15:20:32.676047 IP 10.0.0.1 > 10.0.0.2: ICMP echo request, id 3389, seq 1, length 64
```

https://github.com/Security-Onion-Solutions/securityonion-cloud/tree/dev/vxlan2pcap

MITRE ATT&CK Cloud Matrix

Cloud Matrix

Below are the tactics and technique representing the MITRE ATT&CK® Matrix for Enterprise coverin
Azure, Azure AD, Office 365, SaaS.

Last Modified: 2019-10-09 18:48:31.906000

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Drive-by Compromise	Account Manipulation	Valid Accounts	Application Access Token	Account Manipulation
Exploit Public-Facing Application	Create Account		Redundant Access	Brute Force
Spearphishing Link	Implant Container Image		Revert Cloud Instance	Cloud Instance Metadata API
Trusted Relationship	Office Application Startup		Unused/Unsupported Cloud Regions	Credentials in Files
Valid Accounts	Redundant Access		Valid Accounts	Steal Application Access Token
	Valid Accounts		Web Session Cookie	Steal Web Session Cookie

- Adversary tactics and techniques relative to cloud environments

- Create detections for TIDs through the use of Sigma/Playbook.
- Test detections using ART tests, RTA, or Prelude Operator
- Map coverage with ATT&CK Navigator

https://attack.mitre.org/matrices/enterprise/cloud/

https://github.com/redcanaryco/atomic-red-team

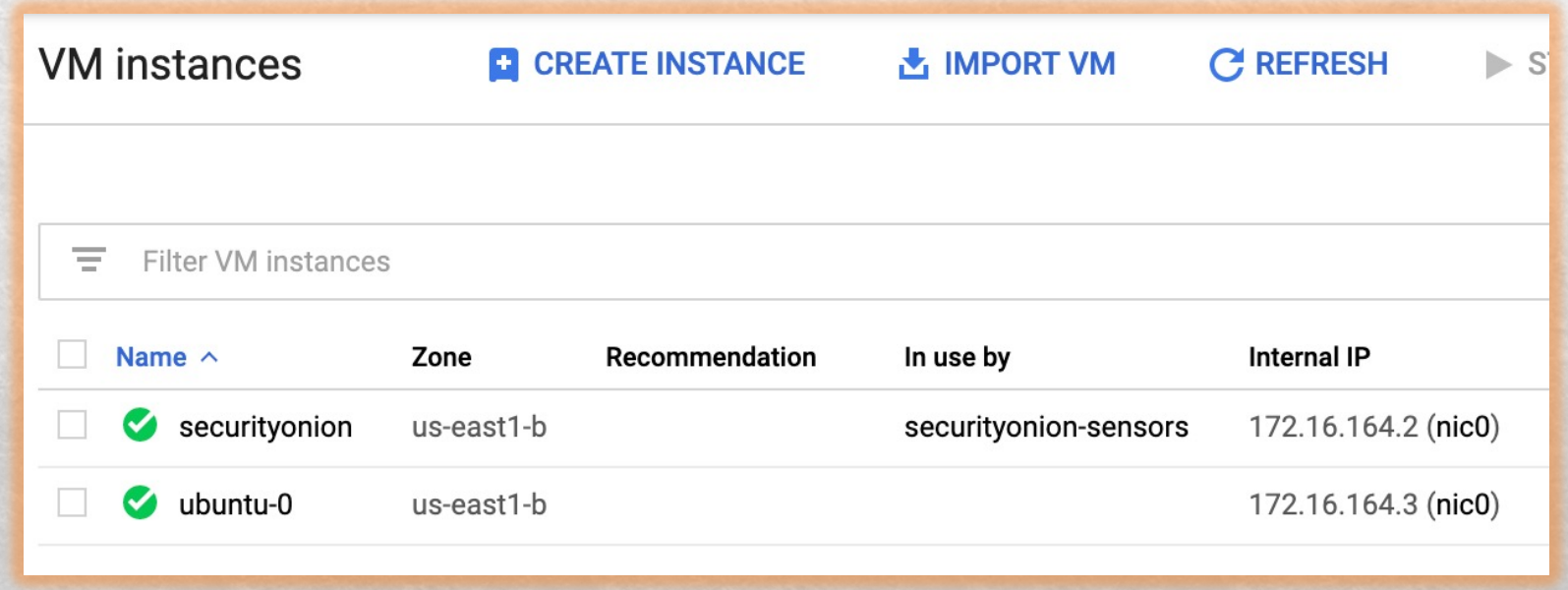
Automated Deployment/Testing

Test AWS Traffic Mirroring and 3CS AutoMirror with Security Onion

- Follow the instructions below to setup a full-fledged VPC that includes:
  - Security Onion
  - Ubuntu/Windows hosts
  - AutoMirror functionality to automatically mirror the traffic for each of the hosts

https://github.com/Security-Onion-Solutions/securityonion-cloud/tree/master/terraform/aws

Test GCP Packet Mirroring with Security Onion



https://github.com/Security-Onion-Solutions/securityonion-cloud/tree/master/terraform/gcp

Contact/Additional Information

@therealwlambert
@securityonion

Download Security Onion

http://securityonion.net/download

Documentation:

https://securityonion.readthedocs.io

AMI:
https://docs.securityonion.net/en/2.3/cloud-ami.html#aws-cloud-ami

Professional Services and Support

https://securityonionsolutions.com

Cloud Resources

http://github.com/security-onion-solutions/securityonion-cloud